Journal of Natural Resources & Environmental Law

Volume 16
Issue 1 *Journal of Natural Resources & Environmental Law, Volume 16, Issue 1*

Article 4

January 2001

A Work Place Surveillance: Who's Watching?

Mark E. Heath
Heenan, Althen & Roles

A WORK PLACE SURVEILLANCE: WHO'S WATCHING?

MARK E. HEATH*

I. INTRODUCTION

At common law, individuals have four basic rights encompassed by the right to privacy:

(1) Protection from commercial appropriation of one's name or likeness;
(2) Protection against public disclosure of private information;
(3) Protection against an invasion of seclusion; and
(4) Protection from being placed in a false light (i.e., having one's opinions misrepresented or misused).[1]

Each of these common law rights has a corollary in the workplace. For example, using an employee in advertisements could be an invasion of privacy -- a violation of the right to be protected from commercial appropriation of one's name or image. Private information about the employee that is maintained by the employer cannot be disseminated without the employee's consent.[2] Employee searches, including bodily searches or searches of workspaces, may be an invasion of an employee's seclusion. If an employer makes statements on behalf of an employee without his consent, he may be placing the employee in a false light in the public eye.[3] Any of these rights can be enforced through civil measures, such as a suit against the employer.

In West Virginia, there is a one-year statute of limitations for an invasion of privacy claim.[4] The claim arises when the plaintiff has actual knowledge of the invasion, not when the plaintiff

---

*Partner, Heenan, Althen & Roles, Charleston, West Virginia. Mr. Heath is a 1986 graduate of the University of Kentucky College of Law and a 1983 *cum laude* graduate of Western Kentucky University. This subject was originally presented at a Cambridge Institute Seminar, *A 1998 Update West Virginia Employment Practical Solutions*. The author would also like to thank Heather Garrison, a third-year law student at West Virginia University School of Law for her assistance in updating this paper for publication.

[1]John F. Buckley and Ronald M. Green, 1999 STATE BY STATE GUIDE TO HUMAN RESOURCES LAW 6-1 (Aspen Publishers 1999 & Supp. 1999).

[2]Gary v. United States, 82 A.F.T.R.2d (RIA) 6964 (S.D. Tenn. 1998).

[3]Buckley and Green, *supra* note 1, at 7-1.

[4]*See* W.VA. CODE § 55-2-12(c) (2000).

reasonably should know, or suspect, that there has been an invasion of privacy.[5] In Kentucky, the statute of limitations for invasion of privacy is one year, using the statute of limitations for libel and slander.[6]

In addition to these common law rights, there are both federal and state statutes governing workplace privacy. These statutes often either level criminal penalties against employers for violations of workplace privacy, or they expand the employee's right to sue his or her employer for an invasion of privacy. This paper will cover these topics in connection with West Virginia cases and statutes, and to the extent possible, Kentucky law.

II. PERSONNEL FILES

A. Disclosure

Many states do not allow employers to disclose information contained in an employee's personnel files to third parties, because such disclosure violates the employee's personal privacy.[7] However, in most states, there are limited exceptions to this rule, such as: (1) limiting the information divulged to name, date of employment, title, and wage paid; (2) divulging information if the employee consents or if a court orders; and (3) divulging information in medical emergencies.[8] In addition, disclosure to government agencies is mandated by law under certain circumstances, such as when the agency is tracking compliance with a law such as the Americans with Disabilities Act (ADA),[9] or the Family Medical Leave Act (FMLA).[10]

As a general rule, disclosing an employee's personnel file to third parties is prohibited unless the disclosure is in the public interest.[11] The public interest varies from state to state. For example, in West Virginia, a financial institution can disclose to other financial institutions that an employee, or former employee, participated in a violation of a federal or state statute or rule.[12] For this to apply, the employee must be applying for a job at the inquiring financial

---

[5]Slack v. Kanawha Housing Authority, 423 S.E.2d 547 (W.Va. 1992).

[6]KY. REV. STAT. ANN. § 413.140(1)(d) (Michie 2000).

[7]9A Individual Employment Rights Manual (BNA) 507:407 (July 1996).

[8]*Id.*

[9]Family and Medical Leave Act of 1993, Pub. L. No. 103-3, 107 Stat 6 (1993).

[10]Americans with Disabilities Act of 1990, Pub. L. No. 101-136, 104 Stat 336 (1990).

[11]Department of the Air Force et al. v. Rose et al., 425 U.S. 352 (1976).

[12]W. VA. CODE § 31A-4-44 (2000).

institution, and the violation must have been duly reported to the appropriate authorities.[13]

Under the ADA, employers may not divulge information about a former employee's disability, illness history, or workers' compensation history to a prospective employer.[14] Employers may, however, divulge information regarding a former employee's job functions and tasks performed by the applicant, the quality and quantity of work performed, how job functions were performed, and any other employment issues that do not relate to the employee's disability.[15] Disclosure of information to third parties will be discussed further in sub-section C.

B. Access

Most states allow employees to have access to their own personnel files, or at least access to documents used to determine qualifications for employment. However, each state is governed by slightly different statutes. In North Carolina, state government employees are entitled to review their personnel record.[16] In Pennsylvania, employees of both public and private employers are entitled to review their own personnel records.[17] The employer may put limits on the review. For instance, the employee can be required to inspect records only during free time, and opportunities for review can be limited to no less than once per year.[18]

In addition to limiting the time and place for review, many states limit the types of information available for review.[19] Usually these limits are prompted by a public policy concern that certain types of information should not be available to individuals because: (1) the information may cause harm to the individual; (2) the information may cause harm to third parties; (3) release of the information may interfere with civil or criminal proceedings; or (4) release of the information would impose undue burdens on the employer.[20] The West Virginia Legislature has not yet addressed these issues. In Kentucky, there is no statutory right to inspect records for private sector employees. Public employees, however,

---

[13] *Id.*

[14] 42 U.S.C.S. § 12112 (Law. Co-op. 2000).

[15] 8 Fair Employment Practice Manual (BNA) 405:7034 (Feb. 1992).

[16] N.C. GEN. STAT. §§ 126-123--126-28 (1999).

[17] PA. STAT. ANN. tit. 43 §§ 1321-1324. (1999).

[18] *Id.* at 1322.

[19] BUCKLEY AND GREEN, *supra* note 4, at 6-5 tbl. 5-2.

[20] 9A Individual Employment Rights Manual (BNA) 507:402 (July 1996).

do have a statutory right to inspect their own personnel files.[21]

Most statutes also regulate whether copies of the personnel files can be made, and whether the employee is entitled to make corrections or insert comments into the records.[22] Federal government employers are required to allow the employee to protest their record, to seek corrections, or to insert an alternative explanation of the facts.[23] In North Carolina, public employees may review and copy any records except for employment references and medical information that a physician feels should not be reviewed.[24] Public employees can follow a specific grievance procedure to have incorrect information removed from their records.[25] However, in Pennsylvania, employees may not copy records and may not review any records relating to the following: an investigation of a criminal offense; references; civil, criminal or grievance procedures; medical records; and materials used by employers to plan future operations or information available to the employee from another source other than the employer (i.e., from a credit bureau).[26] Neither West Virginia nor Kentucky have a private employer statute on this subject.

C. References

Generally, an employer is able, upon request, to give a former employee's prospective employer truthful information about the employee's work conduct. Most states have job reference immunity statutes under which an employer disclosing employment information about job performance to a prospective employer is presumed to be acting in good faith.[27] Although West Virginia has no such legislation at this time, bills regarding employer immunity for dispersing employment information were introduced in the House of Delegates in 1997.[28]

There are limits to an employer's ability to give other employers' information about a former employee under state and federal law, discrimination, retaliation, and blacklisting are prohibited.[29] For example, Title VII[30] has been interpreted to prohibit

---

[21]KY. REV. STAT. ANN. § 18A.020 (Michie 2000).

[22]*Id.*; *see also* N.C. GEN. STAT. § 126-24 (1999).

[23]9A Individual Employment Rights Manual (BNA) 507:402 (July 1996).

[24]N.C. GEN. STAT. § 126-24 (1999).

[25]N.C. GEN. STAT. §§ 125-23 to 126-28 (1999).

[26]PA. STAT. ANN. tit. 43 §§ 1321-1324 (1999).

[27]9A Individual Employment Rights Manual (BNA) 507:409 (July 1996).

[28]*See* HB 2165 (February 20, 1997) and HB 2733 (March 25, 1997).

[29]BUCKLEY AND GREEN, *supra* note 4, 6-5 at tbl. 6.5-1; *see also* Sam's Club v. NLRB, 173 F.3d 233 (4th Cir. 1999) (Michael J., dissenting).

an employer from disseminating adverse references if a discriminatory intent is shown.[31]

An employer must be careful about giving a reference in any situation where a poor reference could be construed as retaliation against someone within a protected class. For example, a public employer cannot retaliate against a "whistle blower."[32] Retaliation could take the form of a poor reference if the employee moves to another job.

West Virginia law also prohibits employers from retaliating against an employee, or former employee, who has filed a complaint or testified in an action under the West Virginia Human Rights Act.[33] If such an employee leaves his or her job and is given a poor reference by the employer, the poor reference could be construed as retaliation against the employee for exercising their rights, which are protected by the Human Rights Act. In addition, state and federal laws prohibit retaliating against an employee for union activities.[34] This includes giving an employee a poor reference based on his union activities.

Blacklisting is generally defined as an employer's preparation, use, or circulation of a list of persons who have been singled out for special avoidance, antagonism, or enmity.[35] Blacklisting someone for union activities is prohibited by the Labor Management Relations Act.[36]

Many states have statutes that specifically prohibit blacklisting.[37] In addition, the statutes usually prohibit an employer from taking any action to prevent a former employee from obtaining employment.[38] Although West Virginia has no statute prohibiting blacklisting, there is case law to suggest that blacklisting is a common law tort in West Virginia.[39] Given the unsettled state of the law, an employer should avoid even the appearance of blacklisting. In Kentucky, the blacklisting of an individual in the mining industry who refuses to deal with, or purchase merchandise from, a specific store is prohibited.[40]

---

[30]42 U.S.C.S. § 2000(e)(1)-(5) (Law. Co-op. 2000).

[31]*See* Kurtis A. Kemper, Annotation, *Dissemination of Adverse Employment References by Former Employer as Unlawful Employment Practice Under Title VII of Civil Rights Act of 1964*, 50 A.L.R. FED. 722 (2000).

[32]W.VA. CODE § 6C-1-3 (2000).

[33]W.VA. CODE § 5-11-9(7)(C) (2000).

[34]Sam's Club v. NLRB, 173 F.3d 233, 239 (4th Cir. 1999).

[35]BUCKLEY AND GREEN, *supra* note 3, 7.5 at 7-51.

[36]29 U.S.C.S § 158 (Law. Co-op. 2000).

[37]BUCKLEY AND GREEN, *supra* note 3, 7.5 at 7-51.

[38]VA. CODE ANN. § 40.1-27 (Michie 1999).

[39]Tiernan v. Charleston, 506 S.E.2d 578, 603 (W. Va. 1998).

[40]KY. REV. STAT. ANN. § 352.550 (Michie 1999).

The West Virginia Supreme Court examined the issue of what an employer can tell another employer about a prospective employee in *Tiernan v. Charleston Area Medical Center*.[41] Betty Tiernan, a nurse, brought suit against her former employer, Charleston Area Medical Center (CAMC), for, among other things, tortious interference with an employment relationship.[42] Ms. Tiernan had been fired from her management position at CAMC for bringing a newspaper reporter to a company meeting.[43] She had a difficult time finding another job in nursing, despite her excellent record at CAMC.[44] After being fired, she worked for several months as a union organizer, then went on to work for a nursing home affiliated with CAMC.[45] After CAMC informed the nursing home that Ms. Tiernan had spent time as a union organizer, Ms. Tiernan was fired from her job at the nursing home.[46] Subsequently, she was unable to find a permanent nursing job.[47]

The majority opinion in *Tiernan* lists the requirements for stating a cause of action for tortious interference with an employment relationship. To make a *prima facie* case, the employee must show (1) the existence of a contractual or business relationship or expectancy; (2) an intentional act of interference by a party outside that relationship or expectancy; (3) proof that the interference caused the harm sustained; and (4) damages.[48]

The employer can offer affirmative defenses in response to a claim for tortious interference with an employee's business relationship. The employer can show that the interference was justified or privileged.[49] For example, the *Tiernan* court stated:

> Defendants are not liable for interference that is negligent rather than intentional, or if they show defenses of legitimate competition between plaintiff and themselves, their financial interests in the induced party's business, their responsibility for another's welfare, their intention to influence another's business policies in which they have an

[41]Tiernan v. Charleston, 506 S.E.2d 578 (W. Va. 1998).
[42]*Id.*
[43]*Id.*
[44]*Id.*
[45]*Id.*
[46]*Id.*
[47]*Tiernan*, 506 S.E.2d 578.
[48]*Id.*
[49]*Id.*

> interest, their giving of honest, truthful, requested advice, or other factors that show the interference was proper.[50]

Most importantly, the *Tiernan* court held that, "In the context of tortuous interference with a business relationship, one who intentionally causes a third person not to perform a contract or not to enter into a prospective business relationship with another does not interfere improperly with the other's relationship by giving the third party (a) truthful information or (b) honest advice within the scope of a request for the advice."[51]

In the employment context, *Tiernan*'s holding makes it unlikely that an employer can be found liable for giving honest references about a former employee. *Tiernan* probably should not be interpreted to give an employer free reign -- it does not given an employer a right to blacklist an employee. However, *Tiernan* does allow an employer to give another employer requested information about a former employee.[52] In his concurrence, Justice McCuskey affirmed the importance of an employer being able to give truthful information about a former employee, characterizing the ability to give a reference as protection of the employer's right to free speech.[53] Deciding this case for Ms. Tiernan would have meant that prospective employee's backgrounds could no longer be checked without the risk of a lawsuit.

Thus, in West Virginia, employers have the right to disclose truthful information about a former employee when solicited by another employer.[54]

III. EMPLOYEE MEDICAL RECORDS

A. Employer Access

Through the Family and Medical Leave Act ("FMLA") employers have access to certain employee medical records.[55] These records must be maintained by the employer in accordance with the ADA requirements for employee privacy.[56]

---

[50]*Id.* at 592.

[51]*Id.*

[52]*Id.*

[53]*Tiernan*, 506 S.E.2d 578 (McCursky, J., concurring).

[54]*Id.*

[55]Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 336 (1990).

[56]411 Fair Employment Practices Manual (BNA) 411:561 (July 1996).

Medical records kept for purposes of FMLA and the ADA must be maintained in confidence -- unauthorized disclosure is prohibited.[57] This applies to current employees, former employees and those who applied for, but were not hired for, positions and were required to take a medical exam after a preliminary offer of employment.[58]

In general, employers must give an employee access to their own medical records maintained by the employer.[59] However, this varies widely by state. Policies range from allowing the employee full access to employer-held medical records, to limiting the employee's access only to information that will not have a detrimental effect on the employee's health.[60] In some states, the employer is not required to divulge any information that the employee could get from a doctor or medical facility.[61]

B. Need to Know

Third-party access to employer-held, employee medical records is strictly limited by federal law.[62] The ADA and the FMLA permit third-party access only when it is necessary.[63] Certain third parties have access to employee medical records because they have a need to know.[64]

Under the ADA, supervisors and managers can access medical records regarding work restrictions and necessary accommodations for employees with disabilities.[65] First aid and safety personnel can access employee medical records if the disability might require emergency treatment.[66]

Federal government officials who are investigating compliance with regulations must be allowed access to employee medical records.[67] Similarly, employers must allow access to state workers' compensation officers or workers' compensation insurance carriers.[68] Under the ADA, employers are permitted to disclose information from employee medical records to their insurance

---

[57] 29 C.F.R. 825.500(g) (2001).
[58] 8 Fair Employment Practices Manual (BNA) 421:908 (Apr. 1998).
[59] 9A Individual Employment Rights Manual (BNA) 507:404 (July 1996).
[60] *Id.*
[61] *Id.*
[62] 8 Fair Employment Practice (BNA) 405:7394 (Sept. 1996).
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] 8 Fair Employment Practice (BNA) 405:7394 (Sept. 1996).

carriers for insurance purposes only.[69]

IV. EMPLOYEE MONITORING

A. Nature of Monitoring

Employer monitoring can be divided into two categories: searches and surveillance.[70] Searches include body searches, workstation searches, vehicle searches, and searches of personal information, among others.[71] Surveillance can be actual or electronic, and can focus on the employee and/or on his work product.[72]

B. Searches

Courts faced with the issue of whether employers should be allowed to conduct searches of employees generally decide the legality of the search based upon balancing the intrusiveness of the search against the need to conduct it.[73]

1. Body Searches

Body searches include, among others, strip searches, pat-downs, drug testing, AIDS testing, and genetic testing.[74] Although there are often no statutes governing a specific type of body search, an employer will usually have to justify a body search with a showing of extreme need.[75] Body searches are the most intrusive kind of search.[76] A court will require a strong showing of employer need to counterbalance the intrusiveness of a body search of any kind.[77] Although the Fourth Amendment does not apply to private employers, an unreasonable body search is still an invasion of the employee's privacy and can give rise to a cause of action.[78]

A West Virginia Supreme Court decision prevents a private sector employer from imposing mandatory drug testing of its employees absent a reasonable, good faith, objective suspicion of the

---

[69] *Id.*
[70] 9A Individual Employment Rights Manual (BNA) 509:701 (Mar. 1998).
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] 9A Individual Employment Rights Manual (BNA) 509:701 (Mar. 1998).
[76] *Id.*
[77] *Id.*
[78] *Id.*

employee's drug use, or absent a legitimate concern for public safety or the safety of other employees.[79] Such testing is contrary to the State's public policy.[80] The court analogized random drug testing to polygraph testing of employees, which had previously been found to be a violation of public policy.[81] The Court found that employer drug testing of employees "portends an invasion of an individual's right to privacy."[82] In the absence of a pre-existing suspicion of the employee's drug use, or of a need to test based on the hazardous nature of the employee's job, drug testing in the workplace violates a substantial public policy in West Virginia, and can be the basis for a lawsuit.[83] There is no statute on this subject in Kentucky.[84] Case law in Kentucky does recognize drug testing based upon "reasonable basis."[85]

There is no statutory authority in West Virginia allowing an employer to demand that an employee take an AIDS test as a condition of obtaining or continuing employment. In addition, in West Virginia, AIDS is considered a handicap.[86] Under the West Virginia Human Rights Act,[87] it is illegal to discriminate against a competent individual on the basis of a handicap.[88] Therefore, even if AIDS testing of potential or present employees were permitted, the employer could not use the results of the AIDS test to distinguish between similarly qualified individuals.[89] In Kentucky, AIDS testing of employees is banned unless it is part of a bona fide occupational qualification.[90] Testing in this area needs to proceed carefully as the Supreme Court now recognizes that having HIV is a handicap.[91]

There are numerous circumstances under which an employer could know the results of an employee's AIDS test,[92] but the employer cannot use this information to discriminate against an

---

[79]Twigg v. Hercules Corp., 406 S.E.2d 52 (W.Va. 1990).

[80]*Id.*

[81]*Id.* at 54.

[82]*Id.* at 55.

[83]*Id.* at 58.

[84]For a good discussion of drug testing in Kentucky, *See* Robert Hudson, *Drug Testing in the Workplace: An Evolving Kentucky Employment Issue.* Kentucky Bench & Bar, Fall 1992, at 14.

[85]*See, e.g.*, Smith v. Kentucky Unemployment Ins. Comm., 906 S.W.2d 362 (Ky. App. 1995); *See also* Cornette v. Commonwealth, 859 S.W.2d 502 (Ky. App. 1995)(testing of bus drivers is also allowed).

[86]Benjamin R. v. Orkin Exterminating Co., 182 W. Va. 615 (1990).

[87]W. VA. CODE § 5-11-1 (1999).

[88]*See* Orkin Exterminating Co., 182 W. Va. 615.

[89]*Id.* at 618.

[90]KY. REV. STAT. ANN. § 207.135 (Michie 1999).

[91]*See* Bragdon v. Abbott, 524 U.S. 624 (1998).

[92]For example, for insurance purposes, to protect other employees and emergency personnel in the event of an accident, etc.

employee.[93] Also, the employee's insurance cannot be terminated, nor can the employer's group insurance policy be terminated, because an individual tests positive for HIV.[94]

2. Searches of Offices and Work Spaces

Public employers generally have wide latitude to search the offices, desks, and files of their employees.[95] The employer is not required to get a warrant to search an employee's work area,[96] and there is no need for the employer to obtain a probable cause determination before performing the search.[97]

The West Virginia Supreme Court has held that a public employer does not need a warrant to search an employee's desk or work area for official property.[98] The employee has no reasonable expectation of privacy in official property, as long as the employee's private property is not subject to search.[99]

This decision has not yet been applied to a private employer. However, in other states, courts have given private sector employers fairly wide latitude to conduct searches of their employees' work areas. For example, when an employer conducted a search after receiving information that employees were storing narcotics on company property and requested that DEA agents be present during the searches, the court found no violation of the employees' right to privacy.[100] Employees should be notified of this right to search workplace desks, offices, and files within an employee handbook.[101]

In another case, a private sector employer obtained police participation in a search for illegal drugs and alcohol stored in an employee's locker.[102] The employer had a reasonable basis for believing that drugs and alcohol were being used at work, and company rules permitted general locker searches.[103] The court found that the employee's privacy had not been violated.[104]

---

[93]Bragdon v. Abbott, 524 U.S. 624 (1998).

[94]W.VA. CODE § 33-16-9 (1987).

[95]O'Conner v. Ortega, 480 U.S. 709 (1987).

[96]*Id.* at 726.

[97]9 Individual Employees' Rights Manual (BNA) 509:702 (Mar. 1998).

[98]State v. Nelson, 189 W. Va. 778 (1993).

[99]*Id.* (employee of Huntington police Department conviction of concealing a third party's criminal record was upheld even though the criminal record was found hidden in a magazine on defendant's desk.).

[100]Melton v. United States Steel Corp., 8 I.E.R. Cases 687 (D.C.N. Ind. 1993).

[101]*Id.*

[102]Faulkner v. Maryland, 564 A.2d 785 (Md. Ct. App. 1989).

[103]*Id.* at 786.

[104]*Id.* at 790.

3. Vehicle Searches

Often, employers may have more reason to search an employee's vehicle than to conduct a body search of the employee. In most cases, the degree of intrusiveness of a vehicle search is relatively low, so employees may not have a cause of action due to searches of their vehicles while the vehicle is on the employer's property.[105]

4. Personal Information

The right to privacy extends to intangibles, including an employee's mental processes.[106] Employers in West Virginia cannot require employees or prospective employees to submit to polygraph or lie detector tests as a condition for retaining or obtaining employment.[107] There are limited exceptions for drug manufacturers, law enforcement, and military forces.[108] The statute is designed to respect an employee's mental privacy, and recognizes that the information sought in a polygraph test can usually be obtained in another less intrusive way, such as a background or reference check.[109]

C. Surveillance

As with searches, the degree to which an employer is liable for surveilling its employees depends on the intrusiveness of the surveillance, balanced against the employer's need to perform the surveillance.[110] Another consideration is the employee's reasonable expectation of privacy.[111] An employee has less expectation of privacy if he knows in advance that surveillance is a condition of employment.[112]

1. Surveillance of Employees

Generally, conducting surveillance of an employee without giving the employee prior notice has been frowned upon in West

---

[105]9 Individual Employment Rights Manual (BNA) 509:707 (Mar. 1998).
[106]Cordle v. General Hugh Mercer Corp., 325 S.E.2d 111, 116 (W.Va. 1984).
[107]*Id.* at 117.
[108]W.Va. Code § 21-5-5 (a), (b) (1996); *Cordle*, 325 S.E. 2d at 117.
[109]*Id.*
[110]*Id.*
[111]*Id.*
[112]*Id.*

Virginia.[113] The courts have held employers liable for an invasion of the employee's privacy where they have videotaped or monitored an employee's activities in the work place.[114]

A West Virginia employer was held responsible for an invasion of an employee's privacy, even though the invasion consisted of another employee placing a listening device in the plaintiff's office without the employer's knowledge or consent.[115] A listening device was placed in the plaintiff's ceiling by her supervisor, who used it to listen in on the plaintiff for several months before she was terminated.[116] The employer, a housing authority, still bore some responsibility for the unlawful surveillance, although it knew nothing about the device, and the device had not been used since the plaintiff's supervisor left.[117] The court may have reached this result because the plaintiff had suspected for some time that her office might be bugged and had complained to the employer on several occasions; however, the employer took no action.[118]

A West Virginia company was enjoined from videotaping its employees while they were in the employee locker room.[119] The camera (there was no audio recording device) was hidden in a fake smoke detector in the ceiling of the locker room.[120] Employees filed a lawsuit after they discovered the camera, and they claimed that their privacy had been invaded.[121] The monitoring was excessive when balanced against the employees' very real interest in privacy in an area such as a locker room.[122] In addition to an injunction, the employees were awarded $75,000 in damages for the invasion of privacy.[123]

In contrast, a California court held that there were no privacy violations under state tort law when an employer placed a video-only camera (no audio) in a county jail's release office without obtaining a warrant.[124] The jail's objectives were lawful and the camera was placed in a non-private office where deputies had a diminished

---

[113]*Id.*

[114]W.Va. Code § 21-5-5 (a), (b); *Cordle* 325 S.E.2d at 117.

[115]Slack v. Kahawk Housing Auth., et al., 423 S.E.2d 543 (W.Va. 1992).

[116]*Id.*

[117]*Id.*

[118]*Id.*

[119]*Id.*

[120]*Id.*

[121]Slack v. Kahawk Housing Auth., et al., 423 S.E.2d 543 (W.Va. 1992).

[122]*Id.*

[123]W.VA. CODE § 21-3-20 (prohibits electronic surveillance of employees in areas designed for health or personal comfort or safeguarding possessions such as restrooms, shower rooms, locker rooms, dressing rooms and employee lounges).

[124]Sacramento County Deputy Sheriff's Ass=n v. Sacramento County, 59 Cal. Rptr. 2d 834, 837 (Ca. Ct. App. 1996).

expectation of privacy.[125] This is distinguishable from the locker room situation, where employees had a substantial interest in privacy. Also, surveillance of a public area with video only was upheld in *Vega-Rodriguez v. Puerto Rico Telephone Co.*[126] This topic continues to be examined by Congress and state legislatures. Senate Bill 984, introduced by Senator Paul Simon (D.-Ill.) in 1993 but not passed, is an example of legislative initiatives to limit electronic monitoring, including computer monitoring and closed circuit television.[127] Recording employee conversations is another area to watch carefully. In West Virginia and Kentucky, at least one of the participants must do the recording or it is illegal.[128]

Surveillance of employees when they are outside the work place has been frowned upon in West Virginia, although such acts are allowed in other states. For example, a West Virginia employer, faced with a Mandolidas suit by an employee who had been injured on the job, hired a private investigator to secretly videotape the plaintiff in the hope of proving that the employee had not been totally disabled by his injury.[129] A magistrate judge ordered the employer to turn the videotape over to the plaintiff employee as part of discovery, since the tapes were direct substantial evidence concerning the physical and mental impairments of the plaintiff.[130]

Other courts have held that there was no invasion of privacy in a similar situation because of the employer's justification for the surveillance. A Michigan court held against an employee when his employer observed him through a camera lens while he was in his home, and when the employer entered his home under false pretenses.[131] The employer had a right to investigate the employee's claimed work-related disability and could do so by these means.[132] Although a West Virginia Court might uphold the surveillance under these conditions, it is unlikely that a West Virginia court would countenance entering an employee's home under false pretenses.

However, in Ohio, a court held that it was a violation of the employee's right to privacy for an employer to search the employee's hotel room, even though the employer had reserved and paid for the

---

[125] *Id.*

[126] 110 F.3d 174 (1st Cir. 1997).

[127] S. 984, 103d Cong., 1st session (1993).

[128] *See* KY. REV. STAT. ANN. § 526.010 (Michie 1999); *See also* Rhodes v. Graham, 37 S.W.2d 46 (Ky. 1931) (tapping telephone line and secretly listening was an invasion of privacy).

[129] *See* Persinger v. Peabody Coal Co., Civil Action No. 5:94-0023 (S.D. W. Va 1995).

[130] *Id.*

[131] Saldana v. Kelsay-Hayes Co., 443 N.W.2d 282, 285 (Mich. Ct. App. 1989).

[132] *Id.*

room.[133] The employee had a cause of action in tort.[134] The employee had a reasonable expectation of privacy, as no business was transacted in the room and the public was not invited in; therefore, the employer had no right to search the hotel room or monitor the employee's activities therein.[135]

Finally, it is illegal in West Virginia, Kentucky, and many other states, to discharge an employee, or refuse to hire an employee, because the employer knows that the employee smokes or uses tobacco products off premises during non-working hours.[136]

2. Surveillance of Computer and E-Mail Databases

In West Virginia, it is illegal to use a computer or computer network to intentionally examine, without authority, any employment, salary, credit, or any other financial or personal information relating to any other person.[137] Although the statute does not clarify whether an employee has any privacy rights when the computer is owned by the employer and used by the employee for work related tasks, it can be presumed that the employee would have very few. The employer is a person in authority –he or she owns and operates the computers or network. Therefore, the employer does not fall in the class targeted by the statute, and is probably able to retrieve and examine any information contained in the computer at will.

In the absence of case law construing the computer privacy statute in the employment context, viability of privacy claims in the area of computers may depend upon the employee's expectation of privacy in the computer. The existence of a reasonable expectation of privacy depends on the facts surrounding each situation, such as whether the employee uses a password to access the computer system, whether employees share a computer, and whether the computer stands alone or is networked into a central system.[138]

Since it is unclear at this point how the law reads, an employer is wise to head off potential privacy litigation before it starts. There are steps that an employer can take in order to be able to monitor an employee's computer or e-mail transmissions with less fear of a lawsuit. First, employers should make sure that employees

---

[133]*See* Sowards v. Norbar, Inc., 605 N.E.2d 468 (Ohio Ct. App. 1992)

[134]*Id.*

[135]*Id.*

[136]W.VA. CODE § 21-3-19(a) (1992); KY. REV. STAT. ANN. § 344.040 (Michie 1997).

[137]W.VA. CODE § 61-3C-12 (Michie 2000).

[138]BUCKLEY AND GREEN, *supra* note 1, 7.6 at 7-69.

know that the e-mail system and individual computer workstations are accessible to the employer, and that the employer will review those files. Second, the employer should make clear when, and under what circumstances, e-mails and computer work stations will be monitored. Third, the employer should take affirmative steps to prevent employees from developing an expectation of privacy in their computer files or e-mails. For example, if an employee has to use a password to access the computer or a network, the employer should make it clear that the use of a password is needed to prevent those outside the office from obtaining access to private files. Thus, such passwords should be used only if justified by security considerations.[139] A network administrator should be able to access all files. The employer may even want to consider informing employees on a regular basis that computer files and e-mails are subject to monitoring.

D. Legislative Attempts to Curb Abuses

There are numerous federal and state statutes that attempt to regulate the extent to which an employer can obtain information about an employee. For example, under the Videotape Privacy Protection Act,[140] it is illegal for a video retailer to disclose information about a customer's videotape rental habits.[141] This area is, therefore, also off limits to employers.[142]

Another example is the Fair Credit Reporting Act,[143] which prohibits employers from obtaining credit reports on current or potential employees without the employee's consent.[144] However, if the employee does not consent to having his or her credit report made available, the employee is not protected by the act from retaliation by the employer.[145]

The Omnibus Crime Control and Safe Streets Act of 1968, amended by the Electronic Communications Privacy Act of 1986,[146] prohibits public and private employers from engaging in surreptitious surveillance of employee activity through the use of electronic devices, especially wiretaps.[147] There are exceptions to

---

[139] *Id.*
[140] 18 U.S.C. § 2710 (2000).
[141] *Id.*
[142] *Id.*
[143] 105 U.S.C. § 1681 (1997).
[144] *Id.*
[145] *Id.*
[146] 18 U.S.C. § 2510 (1999).
[147] *Id.*

this statute that employers should be aware of. The business extension exception permits employers to monitor employees' electronic communications in the ordinary course of business by using any telephone or telegraph equipment provided by its electronic communications service.[148]

Also, if one party consents to the monitoring, an employer can monitor electronic communications between its employees.[149] The party must consent in advance of the monitoring.[150] An employer, thus, can make it clear that employees will be monitored on the telephone or in the e-mail system, and the surveillance can be legitimate.[151] In addition, courts have held that an employee consents to the monitoring if he or she continues to work for the employer after receiving notice that monitoring will start.[152]

1. State Legislation

West Virginia has a Wiretapping and Electronic Surveillance Act, which became law in 1987.[153] Because it is relatively new, there are few cases construing the Act.[154] The Act makes it illegal for any person to intentionally intercept wire, oral, or electronic communications, to disclose information obtained through such interception, or otherwise make use of such information.[155] Any person whose communications are so intercepted or disclosed has a civil cause of action.[156] The Act appears to mirror the federal act in that there is a business exception allowing interception in the normal course of business activities, as well as an exception if one party has given prior consent.[157]

West Virginia Code section 61-3C-12,[158] Computer Invasion of Privacy, provides that:

> Any person who knowingly, willfully and without authorization accesses a computer or

---

[148]18 U.S.C. §§ 2510(4), (5)(a) (1994).

[149]*Id.*

[150]18 U.S.C. § 2511(2)(d) (1999)

[151]*Id.*

[152]*Id.*

[153]W.VA.CODE § 62 1D-1 (2001).

[154]One case has dealt with the admissibility of evidence for illegally obtained evidence. In Wright v. David L., 192 W.Va. 663 (W.Va. 1994), the court ruled that tape recordings illegally made by a grandmother were not admissible in child custody proceedings as, although relevant, they were made in violation of the statute.

[155]W.VA. CODE § 62-1D-3 (1999).

[156]W.VA. CODE § 62-1D-12 (2000).

[157]*See* 15 U.S.C. § 1681(b) (1994).

[158]W.VA. CODE § 61-3C-12.

> computer network and examines any employment, salary, credit or any other financial or personal information relating to any other person, after the time at which the offender knows or reasonably should know that he is without authorization to view the information displayed, shall be guilty of a misdemeanor.

"Authorization" is defined as "the express or implied consent given by another to access or use said person's computer, computer network, computer program, computer software, computer system, password, identifying code or personal identification number."[159]

Although it does not address the issue of employer surveillance of an employee's electronic activities directly, the statute would seem to be fairly permissive. Since the statute is aimed at "hackers,"[160] an employer who owns a computer system or computer network would be considered to have authority to access any information that is stored on it, whether business or personal.[161] However, a separate issue is whether other employees can access the computer system and whether their access might be an invasion of employees' privacy. It would be wise for employers to specify which employees have access to the computer system, and how broad their access may be.

This area requires constant monitoring. Legislation was introduced on this topic in Congress in 1992, but did not pass.[162] California's Governor recently vetoed legislation pending to require notification of employer monitoring.[163]

E. Employers Need to Know

Any litigation involving a search or surveillance of employees requires balancing the intrusiveness of the search or surveillance against the employer's need to conduct the search or surveillance.

To avoid privacy claims, employers should follow several precautions. First, before implementing policies that authorize searches or surveillance of any kind, employers should make sure

---

[159] *Id.*
[160] *Id.*
[161] *Id.*
[162] *See* 9A Individual Employee Rights (BNA) (Sept. 21, 1999).
[163] *Id.*

that their employees know about the policies and understand them. Prospective employees should understand that the searches or surveillance will be part of the conditions of their employment. Employers should take steps to remind employees periodically about the possibility of searches or surveillance. In this way, employees will have a diminished expectation of privacy, and in the event of a claim being filed, a court will be less likely to find an unreasonable invasion of the employee's privacy.

Second, employers should never seek information about an individual's disability, illness, or workers' compensation claim history. When inquiring of other employers or the individual himself, the employer should limit its inquiries to information related to the employee's ability to do a particular job.

Third, if the employer has to maintain sensitive information (i.e., medical records for ADA or FMLA purposes), the employer must ensure that the information is not available to anyone, including other employees, unless they have a need to know the information in order to perform their job duties. Anyone with access to sensitive information should be cautioned to maintain the information in confidence.

Lastly, private employee information should not be disclosed absent authorization from the employee for the disclosure or a substantial reason for the disclosure. This does not mean that an employee cannot provide references to another employer regarding one of its former employees. However, reference information should be confined to the employee's ability to do his job with the former employer. It would be an invasion of privacy to release personal information about an employee to a prospective employer.